TESTIMONY OF

PARRY AFTAB, ESQ.,

The Kids Internet Lawyer, Author and
Child Protection and Cybersafety Advocate

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES,

COMMITTEE ON

EDUCATION AND LABOR

HEALTHY FAMILIES AND COMMUNITIES SUBCOMMITTEE HEARING

Ensuring Student Cyber Safety

10:00 AM, June 24, 2010

2175 Rayburn House Office Building,

Washington, DC

Parry Aftab, Esq.
Parry@Aftab.com
Aftab.com

Cyberbullying, Cybersafety and the Role of Industry in Addressing the Issues

SUMMARY

Cybersafety involves protecting ourselves, our children, our community and our networks. When minors are involved the programs and messages have to be relevant, involve young people in their framing and be quick and easy for parents. Schools often find themselves in the crossfire, especially when cyberbullying among students or sexting images arise. At the same time, the power of digital networks and interactive technology to spur creative educational methods and engage students, parents and educators in forward-thinking ways means we can't sink our heads in the sand and have to find a way to balance the benefits while containing the risks.

If we view cybersafety as a risk-management issue, it is often easier to tackle. It includes copyright infringement and plagiarism, responsible use, information literacy, digital literacy and digital hygiene, privacy, security, misinformation and hype, sexual exploitation (including the rapid growth of sexting), cyberbullying, ID theft and inappropriate, violent and sexual content.

While my books and non-profit role, as Executive Director and Founder of WiredSafety.org, span all risks for consumers and families online, my particular passion is the prevention and ways to address cyberbullying. I created StopCyberbullying.org to help parents, schools, students, law enforcement and all stakeholders address the growing problem of children hurting each other online.

To address cyberbullying adequately, in addition to understanding the stakeholder perspectives, we have to develop educational programs and materials, awareness of the issue and help for victims and their families. We have to focus on character education, role modeling good behaviors for our children and ways to get everyone involved and informed.

We also have to make it easier to understand the scope of the risks and solutions to those risks. When it comes to addressing a big problem from multiple perspectives, industry's involvement is crucial and welcome. Over the years the Internet, technology and offline trusted family brands have stepped up to the plate to help design programs, materials and resources, provide expertise and distribute them to their communities online and offline. Their approaches are as varied as their businesses. And our children are safer and our parents better informed because of their involvement.

Offline and online resources and intervention points tying the schools together with industry and community organizations, as well as the families they serve, must be developed and adopted. We need a cybersafety ecosystem that addresses the most common as well as the most serious risks, and we can continue to look to the technology, entertainment, device and software manufacturers, service providers and Internet industry as advisors for their valuable help.

OPENING STATEMENT

Defining the Cyberbullying Problem[1]

We can't address a problem until it is defined. While there are several attempts to define "cyberbullying" as more than "you'll know it when you see it," WiredSafety defines it as when minors use digital technology as a weapon to hurt another minor. We have been doing this since 1995, longer than any other group, and find that this definition is practical, realistic, and separates adult cyberharassment from minor-to-minor attacks. To meet WiredSafety's definition of cyberbullying, the actions must be intentional, minor-to-minor and must use some type of digital technology (cell phones, Internet, social networks, gaming devices, IM, email, images, YouTube, virtual worlds/games, etc.). The actions can range from a one-time serious threat to repeated and unwanted insults, can be conducted as direct one-to-one attacks (direct cyberbullying), postings intended to be viewed by many (indirect cyberbullying) or schemes designed to set up the victim and have someone else do their dirty work (parents when the text bill arrives, Facebook when false reports are made to them, etc.).

Cyberbullying is growing in epidemic proportions- just ask any middle school teacher, counselor or principal. Over the last two years the number of kids experiencing cyberbullying has increased by more than 30% with attacks becoming increasingly more hateful and vicious. It is also starting earlier and earlier as first and second graders are getting online and stealing virtual world and online games points and passwords from their friends and classmates.

However, children's' motives and methods change as they get older and often by gender. Boys tend to use technology tools and infiltrate accounts (hack) or threaten their targets, while girls tend to use social exclusion and reputational attacks. Unlike in face-to-face bullying, size and gender are often irrelevant: girls cyberbully boys, boys cyberbully girls, smaller kids cyberbully the big tough ones. Technology levels all playing fields. As a result, the only way to tackle the problem of cyberbullying is to combine all stakeholders and to be as inventive as children who cyberbully. In short, we need to find what works and seek solutions everywhere, from everyone. We have to think outside of the box.

Educating Students to Stop Cyberbullying

Industry has an important stake in both keeping children and teens safe online and educating parents and their communities. Fortunately, leaders and newcomers alike are interested, involved and generous in sharing their expertise, funding and access. I founded and run WiredSafety, a charity that began its work in 1995 through its unpaid and loosely-organized volunteers by rating websites and helping victims of cyberabuse and cybercrime online; in 15 years there is little we haven't encountered, but cyberbullying and cyberharassment prevention and help is one of our core missions. When I wrote StopCyberbullying.org several years ago as a joint project with WiredSafety, it quickly became the most popular cyberbullying awareness site online. Families, schools and communities needed help grappling with this growing problem, and StopCyberbullying.org delivered what they needed.

This September, WiredSafety and I will release the StopCyberbullying Toolkit I authored in time to help students and educators headed back-to-school. The Toolkit contains $1 million worth of animations, computer games, lesson plans and classroom activities, videos, posters, coloring sheets and worksheets,

[1] I have attached information about cyberbullying, how it works and ways to address it in the Appendix, along with my one-page bio.

guides, tip lists and community campaigns for educators, parents, school administrators, guidance counselors, school resource officers and community policing agents, parent teacher organizations and K-12 students. It is a single free downloadable resource for US schools that can be customized to address local and regional concerns and students with special needs. How can a million dollar resource be developed and distributed for free without government funding? We turned to the industry for help and they responded in droves.

Microsoft, Facebook, MySpace and LG Phones joined as platinum sponsors. AOL, Procter & Gamble, Spectorsoft, myYearbook, KidZui, Build-A-Bear Workshop and others also joined as sponsors. The Girl Scouts of the USA, National Crime Prevention Council, ADL, Rachel Simmons, Michele Borba, Bonnie Bracey, Art Wolinsky, Dr. Deanna Guy, Dr. Tom Biller, Teenangels and Tweenangels, Cynthia Logan, Debbie Johnston, Chris Hansen, XBox, Disney, WebKinz, Zynga, Yahoo!, Nickelodeon, MTV, Pantilla Amiga, Adobe, Unity, Pace University, McAfee, Verizon, Nokia, MiniClip, Candystand (FunTank), Dolphin Entertainment, Hearst, Conde Nast, Seventeen Magazine, ToysRUs, Readers Digest, People Magazine, YouSendIt, the Child Safety Research and Innovation Center, WiredTrust, Marvel and vast numbers of others contributing expertise, support and in-kind to help create and distribute this multi-stakeholder resource with the best available content and activities available.

The charity I run in volunteer-capacity, WiredSafety, also works to bring together all stakeholders through summits, conferences and events sponsored by industry leaders. The first International Stop Cyberbullying Summit was hosted by WiredSafety in 2008 and Verizon's Chairman and CEO, Ivan Seidenberg, delivered the luncheon speech to explain how committed Verizon is to stopping cyberbullying. Since then, they have been important leaders in the industry and brought together other stakeholders to help address the problem. LG Phone and Nokia are becoming engaged in cybersafety messaging and educating the parents who buy their products for their children.

Many other industry players have joined forced with us as well as worked on their own to create programs and raise awareness about cyberbullying. For example:

- Facebook is developing a cyberbullying and harassment page in its safety section to teach parents, teens and users of all ages how to avoid becoming a victim of cyberbullying or being seen as a cyberbully. They have revised their privacy settings to help keep cyberbullies from abusing users' information and posing as them. (The more a network authenticates a user, the less likely cyberbullying can gain ground.) Recently, Facebook partnered with the National Parent Teacher Association to help deliver cyberbullying and other programs to parents at the local level and share wonderful resources and information from the National PTA with others on Facebook. They have also committed the help of their five chosen safety advisory board members (including WiredSafety).
- McAfee partnered with Facebook to provide free long-term trial security software products to all Facebook users. By using a good security product, cyberbullies can be locked out of computers, devices and accounts.
- ToysRUs is partnering with me and WiredSafety's Tweenangels, WiredMoms to develop information for parents about different interactive toys and devices and how to make the right choice for their children. This will involve in-store information, online tutorials and content, and

training and engagement of their employees, as well as Tweenangel and WiredMoms reviews of their favorite products.

- XBox and Microsoft have developed the Pact, a contract for parents and their children that addresses time spent playing games and using media and rules. The Pact can be customized for each family and each child. They have also created an advisory board that includes one of our Teenangels and me.
- MTV's A Thin Line campaign started with a survey on teens and young adult practices and risks related to sexting and cyberbullying. A documentary program on the consequences of sexting for both those taking the nude picture and those forwarding it was broadcast with a wide viewership. The athinline.org site engages young people and challenges them to take charge. It informs them what to do when they encounter cyberbullying, how to respect themselves and others and how to tell when their actions and those of others have "crossed the line." They address cyberspying by friends and romantic partners and the right of privacy.
- Seventeen Magazine has announced a large campaign to activate and empower youth especially girls and young women, to tackle cyberbullies and step up when they see others being harmed online. I will be working with them on this campaign, as will my Teenangels
- Liz Claiborne expanded its free dating abuse campaign and curricula to include digital dating abuse, asking me to create that segment of the curricula (loveisnotabuse.org).
- Taser International is creating cybersafety and cyberbullying training and resources for members of law enforcement using their certified trainers. They are also helping develop resources for local law enforcement agencies and community policing agents to use in delivering programs to their communities on cybersafety and cyberbullying. Having learned about the concerns parents and the law enforcement community had addressing distracted driving risks and cyberbullying and other cell phone-related abuses, Taser developed a cell phone and in-car technology to prevent driver cell phone and other distractions and to give parents better control and ability to supervise their children's cell phone activities, including prohibiting the sharing of "sext" images and receipt of phone calls from strangers. The two products will be released this year and are part of a broader campaign to address risks to our families.
- Microsoft Window funded a comprehensive cybersafety and cyberbullying awareness and educational initiative for the Girl Scouts of the USA entitled "Let Me Know" or "LMK" developed by me using our Congressionally-honored Teenangels program as the model. (This is intended to serve the 2 million plus members of Girl Scouts.)
- The gaming companies, such as Lego, FunTank (Candystand.com), Zynga, Disney, Nickelodeon, and Nintendo are developing technologies and methods to better protect their users of all ages. Specifically, Nickelodeon is teaching parents and young users how to use games and online networks in safer ways and to avoid being the target of a cyberbully. Zynga (of Farmville and Mafia Wars fame) is developing safety messaging on game bullying , security and safety with WiredSafety and with me. Nintendo added parental controls to its DSi to help parents better address their concerns.
- Disney uses its TV programming and product messaging to teach safer web surfing and cyberbullying prevention, including on its netbooks and Club Penguin. Disney has created a corps of kids who act as "secret agents" to Club Penguin to spot cyberbullying and other code of conduct violations in the game. I worked with them on a segment of HGTV's Designing Spaces

where I appeared helping a Florida parent understand the best way to create a "cybersafe" room for her son and together with Teenangels in 1998 helped design Toowtown's safety features.

- The community approach, where the millions of users are engaged in looking out for themselves and others, is becoming more robust and filters adopted by Build-A-Bear Workshop help prevent their younger users of buildabearville.com from targeting each other. They partnered with us in StopCyberbullying month last year, offering in-store materials for parents and pledges for children and added a "stop, block and tell!" move in their game to help make cyberbullying awareness fun. They are founding members of the StopCyberbullying Coalition and Maxine herself blogs to her millions of fans about what parents need to know to keep their kids safer.
- KidZui is delivering our Sumo-Wrestler Panda Cybersafety animations, teaching children how to avoid and respond to cyberbullying.
- AOL is heavily involved in supporting mom digital literacy and awareness and is a sponsor of WiredMoms, WiredSafety's mom group with more than 70,000 followers on Twitter (@wiredmom and @wiredmoms)
- Cisco commissioned us to create cybersafety guides for kids, tweens, teens and parents for promotion on their sites and other sites online.
- Ceridian and IBM commissioned me to create a tour of the teens' Internet for parents in video and podcast/audio formats as an employee benefit for IBM employees worldwide and US military families.
- Microsoft sponsored the development of the Alex Wonder Kid CyberDetective Agency Bootcamp Computer Game, teaching tweens how to identify and address cyberbullying as well as our first Marvel Internet Superheroes Comic on cyberbullying.
- In 2004, Marvel donated an exclusive license to use Spiderman, The Incredible Hulk and others in their Superhero studio in comics offering cybersafety, security and digital technology-related issues.
- Adobe donates expertise to us on special-needs accessibility to allow for adaptation of cybersafety materials and resources for the families of special-needs children and the children themselves.
- Google and Yahoo! support public service messaging and search promotions to select Internet child safety advocacy groups.
- Oracle operates Think.com, a popular educational resource for educators on digital use and empowerment.

Socially Safety

Finally, many general audience industry leaders have started to provide cyberbullying training for their moderators and address cyberbullying risks through programs and policies. In the case of those sites designed exclusively as tween and preteen networks, in addition to complying with COPPA, many are delivering materials to parents and schools, as well as resources directed to their preteen audiences. The *Socially Safe Best Practice Seal* and the *Socially Safe Kids Seal* are providing a framework for safety, best practices and risk-management to the Internet, online game and digital technology provider industries. In addition we are delivering training and certification programs for moderators and, together with privacy and security think tank experts, will launch *Pathway*, a screening and moderation

technology for use by networks, game sites and technology providers to help monitor their services and deliver a safer environment and experience. These steps go a long way to help professionalize Internet safety and best practices.

This new approach of branding safety and best practices works because, in addition to being good for communities, families and schools, keeping all users, especially children safer is also good for business. Trusted brand names and responsible newer companies recognize these opportunities and their responsibilities to their customers, users and the community.

A representative of Google, while speaking at one of our StopCyberbullying Coalition events, stated that creating safer networks is "an issue of competition." If your competitors are helping make things safer, you have to as well. That was welcomed news.

But while it may be a competitive advantage to make your networks and technologies safer, it also makes sense to join forces with and cooperate with your competition and all industry players to create safer online environments and better prepared young people and parents. An example on how they are working together for the good of all Internet and digital technology users is our StopCyberbullying Coalition. The StopCyberbullying Coalition is a multi-stakeholder group organized by WiredSafety and run by me to bring together all viewpoints and expertise to tackle this growing problem from all perspectives. Without the creativity, access, distribution channels and support of the above- mentioned companies and many more, non-profits, schools and families would not have the help they need to address cyberbullying, cyberhate and the harassment of minors in the digital world.

CONCLUSION

Thank you for including my testimony on this critically important issue for our nations' youth. Cyberbullying is reaching epidemic proportions, touching kids at every age and grade level. Thankfully many within industry, schools and communities have begun to answer the call to provide training programs, materials, and educational efforts to "Stop Cyberbullying". I stand ready to answer any questions the Subcommittee may have and provide additional information and offer the support of both WiredSafety and its thousands of volunteers.

APPENDIX TO TESTIMONY OF PARRY AFTAB, ESQ.

SNAPSHOT OF U.S. MINORS ONLINE AND CYBERBULLYING

It is estimated that approximately 93% of minors in the Unites States 10 and older access the Internet either from home, schools, community centers and libraries or from some newer Internet-capable device. This is up more than fifteen-fold since 1996, when only 6 million U.S. minors were online. Now our children are using cell phones with video and camera features as well as Internet and text-capability, iTouches and iPads with cell phone-like features, interactive gaming devices (such as XBox and Sony Playstation 3) with voice-over-Internet , webcams and live chat features, handheld devices with Internet, Bluetooth and other remote-communication technology (such as DS and DSi), community broadcasts like Twitter and social networking profiles (such as Facebook, MySpace and myYearbook) where they can share their thoughts, when they last brushed their teeth, and anything else they want the world (or their closest friends) to know.

Fifteen years ago, when our volunteers first began helping victims of cyberbullying and cyberharassment things were easier. There was one way to access the Internet – a computer with a slow dial-up modem. The Internet was too rare and access to expensive for kids and teens to use and "central locations[2]" where parents could oversee their kids' surfing made sense. But this has changed radically over these few short years. Now our kids and teens have more power in their backpacks, pockets and purses than large corporations had a few years ago. They have "apps" for everything, change their status on Facebook, share pictures on Flickr, Tweet, upload videos on YouTube, send thousands of texts (and sometimes "sexts") and live out-loud online.

Now, instead of looking over our children's shoulders when they are connected, we have to teach our children to use the "filter between their ears" and exercise good judgment and care when using any interactive device wherever they are and however they are connected. While teaching parents how to supervise their children online was a challenge, teaching children to "ThinkB4uClick" is much harder.

When I was growing up (in the days before electricity and indoor plumbing, when we had to walk up hill, both ways in blizzards to get to school), parents used to blame us for not behaving. We were disciplinary problems. Now pediatric neuro-psychologists tell us that preteens and teens are hardwired, through immature brain development, to be unable to control their impulses at this age. Either way, we recognize that preteens and teens take risks, don't appreciate the consequences of their actions and act before they think. This puts them at risk for many things, including, but not limited to being cyberbullied or being the cyberbully. (Often the only difference between the two is which clicked the mouse last.)

[2] Thirteen years ago, when I first wrote the first book in the world on Internet safety for parents and told them to put the computer in a "central location," that made sense. It was a central point, where parents could get involved and supervise their children's interactive communications and surfing activities. Now, where they are connected through handheld devices, cell phones and game boxes, it is no longer relevant.

In middle school and elementary school, we call it "cyberbullying." High schoolers think that "cyberbullying" is a middle school thing and they are too mature for it. They call the same activities that constitute "cyberbullying" "digital drama" or "digital abuse." [3]

Statistics and a Snapshot of Cyberbullying Trends

A few years ago, I visited schools around the U.S. doing presentations to students in elementary, middle and high schools. During each presentation, I asked students if they had been cyberbullied. Instead of asking that way, since each student defines cyberbullying in different ways, I listed the kinds of things that constitute cyberbullying, asking if they had experienced any of those. (They included having someone access your profile, posting something hateful and then changing your password so you can't remove it, passing vicious rumors, posing as you and saying mean things to your friends or breaking up with your girlfriend or boyfriend, etc.) I spoke to a total of more than 44,000 middle school students and no matter where I went in the U.S.; I never found less than 85% of the students reporting that they had been cyberbullied at least once. In a much smaller poll, 70% of the students polled admitted to having cyberbullied someone else at least once. Students are inventive and cyberbullying is often a "crime of convenience, "committed when they are bored, jealous, vengeful or looking for an audience.

Cyberbullying spans all digital technologies, from cell phones where students may grab an unattended cellphone and reprogram the victim's best friend's or romantic interest's number to their cell number. Then they send a mean text message that would come up as the best friend or a break-up message ostensibly from their girlfriend or boyfriend. The victim would blame their friend and two students are victimized for the price of one cyberbullying tactic. (They should spend half the time studying as they do dreaming up these kinds of schemes!)

Key Statistics on Cyberbullying from StopCyberbullying.org and Teenangels

- 85% of middle schoolers polled reported being cyberbullied at least once.
- 70% of teens polled reported cyberbullying someone else.
- 86% of elementary school students share their password with their friend(s).
  70% of teens polled said they share their password with their boyfriend/girlfriend or best friend. (Sharing your password is the digital generation's equivalent of a "friendship ring.")
- Cyberbullying starts in 2nd - 3rd grade and peaks in 4th grade and again in 7th-9th grade.
- Only 5% of middle schoolers would tell their parents if they were cyberbullied.
- Middle schoolers have identified 63 different reasons not to tell their parents.
- Teens have identified 71 different ways to cyberbully someone.
- Cellphones are used 38% of the time in cyberbullying incidents.
- Social networks are used 39% of the time in cyberbullying incidents.
- Password theft or misuse accounts for 27% of cyberbullying. (There is overlap between this and social networking cyberbullying.)
- The number of cyberbullying and sextbullying (when sexting incidents are used to intentionally destroy a minor's reputation and self-esteeem) is increasing rapidly.
- 52% of boys in high school reported having seen at least one nude image of a classmate.

[3] MTV's wonderful multi-year campaign to address cyberbullying, digital dating abuse and sexting risks was launched in late 2009 and can be found at athinline.org. It explains the scope of the teen and young adult issues. I serve as a member of its advisory board, along with Casi Lumbra, one of my Teenangels.

- 1000 Wisconsin teens identified cyberbullying as a risk or a serious risk.
- An equal percentage of boys and girls admit to taking and sharing a sext of themselves.
- 71% of girls use their webcam in their bedroom, and 21% regret something they did on a webcam.
- 5% of 10 – 12 yr olds polled admitted to taking and sharing a sexually provocative or nude photo of themselves.
- Within a 48 hour period, more than 200,000 myYearbook users took a pledge against cyberbullying.

What are the Different Types of Cyberbullies?

It is impossible to change behavior when no one understands what is behind it. Cyberbullying occurs for the same reasons schoolyard bullying occurs. It also occurs by accident when students are careless about cyber communications. It might come from impulsive and thoughtless reactions to something that has upset the "cyberbully." They may be defending themselves and each other from offline bullies or other cyberbullies. Lumping them all together will lead nowhere, fast.

Every Type of Cyberbullying Requires a Different Response and Method of Prevention

The four types of cyberbullies include:

- The Vengeful Angel
- The Power-Hungry (or Revenge of the Nerds sub-type)
- The Mean Girls
- The Inadvertent Cyberbully

"The Vengeful Angel": In this type of cyberbullying, the cyberbully doesn't see themselves as a bully at all. They see themselves as righting wrongs, or protecting themselves or others from the "bad guy" they are now victimizing. The Vengeful Angel cyberbully often gets involved trying to protect a friend who is being bullied or cyberbullied. They generally work alone, but may share their activities and motives with their close friends and others they perceive as being victimized by the person they are cyberbullying.

Vengeful Angels need to know that no one should try and take justice into their own hands. They need to understand that few things are clear enough to understand, and that fighting bullying with more bullying only makes things worse. They need to see themselves as bullies, not the do-gooder they think they are. It also helps to address the reasons they lashed out in the first place. If they sense injustices, maybe there really are injustices. Instead of just blaming the Vengeful Angel, solutions here also require that the situation be reviewed to see what can be done to address the underlying problem. Is there a place to report bullying or cyberbullying? Can that be done anonymously? Is there a peer counseling group that handles these matters? What about parents and school administrators. Do they ignore bullying when it occurs, or do they take it seriously? The more methods we can give these kinds of cyberbullies to use official channels to right wrongs, the less often they will try to take justice into their own hands.

The "Power-Hungry" and "Revenge of the Nerds": Just as their schoolyard counterparts, some cyberbullies want to exert their authority, show that they are powerful enough to make others do what they want and some want to control others with fear. Sometimes they just don't like the other kid. These are no different than the offline tough schoolyard bullies, except for their method. Power-Hungry cyberbullies usually need an audience. It may be a small audience of their friends or those within their circle at school. Often the power they feel when only cyberbullying someone is not enough to feed their need to be seen as powerful and intimidating. They often brag about their actions. They want a reaction, and without one may escalate their activities to get one.

Interestingly enough, a sub type of the Power-Hungry cyberbully is often the victim of typical offline bullying. They may be female, or physically smaller, the ones picked on for not being popular enough, or cool enough. They may have greater technical skills. Some people call this type the "Revenge of the Nerds" cyberbully. It is their intention to frighten or embarrass their victims. And they are empowered by the anonymity of the Internet and digital communications and the fact that they never have to confront their victim. They may act tough online, but are not tough in real life. They are often not a bully but "just playing one on TV."

This kind of cyberbullying usually takes place one-on-one and the cyberbully often keeps their activities secret from their friends. If they share their actions, they are doing it only with others they feel would be sympathetic. The rarely appreciate the seriousness of their actions, and often resort to cyberbullying-by proxy. Because of this and their tech skills, it can be the most dangerous of all cyberbullying.

Power-Hungry cyberbullies often react best when they know that few things are ever anonymous online. We leave a trail of cyber-breadcrumbs behind us wherever we go in cyberspace. And, with the assistance of a law enforcement or legal subpoena, we can almost always find the cyber-abusers and cybercriminals in real life. Shining a bright light on their activities helps too. When they are exposed, letting the school community know about their exposure helps prevent copycat cyberbullying.

Helping them to realize the magnitude of their activities is also helpful. Often their activities rise to the criminal level. The more this type of cyberbully understands the legal consequences of their actions, the more they think about their actions.

Ignoring them can also be very effective. But sometimes, instead of going away when ignored, they escalate their actions to get others involved, through a cyberbullying-by-proxy situation. Whenever a Power-Hungry cyberbully is suspected, it is crucial that law enforcement is notified and that the victim keeps a careful watch on themselves online, through "googling themselves." They can even set a Google Alert to notify them by e-mail if anything new is posted online with their personal contact information.

"Mean Girls": The type of cyberbullying occurs when the cyberbully is bored or looking for entertainment. It is largely ego-based and the most immature of all cyberbullying types. Typically, in Mean Girls bullying situations, the cyberbullies are female. They may be bullying other girls (most frequently) or boys (less frequently).

Mean Girls cyberbullying is usually done, or at least planned, in a group, either virtually or together in one room. It may occur from a school library or a slumber party or from the family room of someone after school. This kind of cyberbullying requires an audience. The cyberbullies in a Mean Girls situation want others to know who they are and that they have the power to cyberbully others. This kind of cyberbullying grows when fed by group admiration, cliques or by the silence of others who stand by and let it happen. It quickly dies if they don't get the entertainment value they are seeking.

The most effective tool in handling a Mean Girls cyberbullying case is blocking controls. Block them, block all alternate screen names and force them to go elsewhere for their sick entertainment. In addition, if threatened with loss of their Facebook or AIM accounts, they wise up fast!

In all cases of which I am aware, the sexting and cyberbullying-suicides and attempted suicides in the US involved Mean Girls cyberbullies.

The "Inadvertent Cyberbully": Inadvertent cyberbullies usually don't think they are cyberbullies at all. They may be pretending to be tough online, or role playing, or they may be reacting to hateful or provocative messages they have received. Unlike the Revenge of the Nerds cyberbullies, they don't lash out intentionally. They just respond without thinking about the consequences of their actions.

They may feel hurt, or angry because of a communication sent to them, or something they have seen online. And they tend to respond in anger or frustration. They don't think before clicking "send."

Sometimes, while experimenting in role-playing online, they may send cyberbullying communications or target someone without understanding how serious this could be. They do it for the heck of it "Because I Can." They do it for the fun of it. They may also do it to one of their friends, joking around. But their friend may not recognize that it is another friend or may take it seriously. They tend to do this when alone, and are mostly surprised when someone accuses them of cyberabuse.

They also may be careless, typing too fast and being unclear or leaving our crucial words, like "not." They may send a message to the wrong person or hurt someone by accident.

Education plays an important role in preventing Inadvertent Cyberbullying. Teaching them to respect others and to be sensitive to their needs is the most effective way of dealing with this kind of cyberbully. Teaching them to Take5! is an easy way to help them spot potentially bullying behavior before it's too late.

Methods of Cyberbullying

Kids have always tormented each other. Just think about *Lord of the Flies.* Now with the help of cybertechnologies, sadly, they are doing it more and more online, using mobile phones and interactive games. I spend as much time protecting kids from each other online these days as from cyberpredators.

What is Cyberbullying?: Cyberbullying is any cyber-communication or publication posted or sent by a minor online, by instant messenger, e-mail, website, diary site, online profile, interactive game, handheld device, cell phone or other interactive device that is intended to frighten, embarrass, harass or otherwise target another minor. If there aren't minors on both sides of the communication, it is considered cyberharassment, not cyberbullying. A one-time rude or insulting communication sent to a minor is generally not considered cyberbullying. Cyberbullying needs to be repeated, or a threat of bodily harm, or a public posting designed to hurt, embarrass or otherwise target a child.

How does it work?: There are two kinds of cyberbullying: direct attacks (messages sent to your kids directly) and cyberbullying by proxy (using others to help cyberbully the victim, either with or without the accomplice's knowledge). Because cyberbullying by proxy often gets adults involved in the harassment, it is much more dangerous.

Direct Attacks

1. Instant Messaging/E-mail/Text Messaging/Inbox or PM Harassment

2. Kids may send hateful or threatening messages to other kids without realizing that unkind or threatening messages are hurtful and very serious.

3. Warning/Report Abuse/Notify Wars—Many Internet Service Providers offer a way of reporting or "telling on" a user who is saying inappropriate things. Kids often engage in "warning wars" which can lead to kicking someone offline for a period of time. While this should be a security tool, kids sometimes use the Warn/Notify/Report Abuse buttons as a game or prank.

4. A kid/teen may create a screen name that is very similar to another kid's name. The name may have an additional "i" or one less "e." It might use a lowercase "L" instead of the number "1." They may use this name to say inappropriate things to other users while posing as the other person.

    a. Text wars, text-bombs, or text attacks occur when kids gang up on the victim, sending thousands of text messages to the victim's cellphone or other mobile device. The victim is then faced with a huge cellphone bill and angry parents.

    b. Kids send death threats using IM and text messaging as well as photos/videos (see below).

Stealing Passwords

    a. A kid may steal another child's password and begin to chat with other people, pretending to be the other kid. He/she may say mean things that offend and anger this person's friends or even strangers. Meanwhile, the others won't know it is not really that person they are talking to.

b. A kid may also use another kid's password to change his/her profile to include sexual, racist, and inappropriate things that may attract unwanted attention or offend people.

c. A kid often steals the password and locks the victim out of their own account.

d. Once the password is stolen, hackers may use it to hack into the victim's computer.

e. A stolen password can allow the cyberbully to steal points, loot, and game "gold."

Blogs

Blogs are online journals. They are a fun way for kids and teens to post messages for all of their friends to see. However, kids sometimes use these blogs to damage other kids' reputations or invade their privacy. For example, in one case, a boy posted a bunch of blogs about his breakup with his ex-girlfriend, explaining how she destroyed his life and calling her degrading names. Their mutual friends read about this and criticized her. She was embarrassed and hurt, all because another kid posted mean, private, and false information about her. Sometimes kids set up a blog or profile page pretending to be their victim and saying things designed to humiliate them.

Websites

a. Children used to tease each other in the playground; now they do it on websites. Kids sometimes create websites that may insult or endanger another child. They create pages specifically designed to insult another kid or group of people.
b. They select and register domain names designed to inflame or otherwise hurt their victims.

c. Kids also post other kids' personal information and pictures, putting those people at a greater risk of being contacted or found.

Sending Pictures Through E-mail and Cellphones

a. There have been cases of teens sending mass e-mails to other users that include nude or degrading pictures of other teens. Once an e-mail like this is sent, it is passed around to hundreds of other people within hours. There is no way of controlling where it goes.

b. Many of the newer cellphones allow kids to send pictures to each other. The kids receive the pictures directly on their phones and may send them to everyone in their address books. After viewing the picture at a website, some kids have actually posted these often pornographic pictures online for anyone to see, spread, or download.

c. Kids often take a picture of someone in a locker room, bathroom, or dressing room and post it online or send it to others on cellphones.

Internet Polling

Who's hot? Who's not? Who is the biggest slut in the sixth grade? These types of questions run rampant on the Internet polls; all created by yours truly—kids and teens. Such questions are often very offensive to others and are yet another way that kids can bully other kids online.

Interactive Gaming

Many kids today are playing interactive games on gaming devices such as Xbox 360 and Sony PlayStation 3, Nintendo DS, and Sony PSP. These gaming devices may allow students to communicate with anyone they find themselves matched with in an online game or people within a certain defined physical area. Sometimes the kids verbally abuse the other kids, using threats and lewd language. Sometimes they take it further, locking them out of games, passing false rumors about them, or hacking into their accounts.

Sending Malicious Code

Many kids will send viruses, spyware, and hacking programs to their victims. They do this to either destroy their computers or spy on their victim. Trojan horse programs allow the cyberbully to remotely control their victim's computer and can be used to erase the victim's hard drive.

Sending Porn and Other Junk E-mail and IMs

Cyberbullies often will sign up their victims for e-mail and IM marketing lists, lots of them, especially porn sites. When the victim receives thousands of e-mails from pornographers, their parents usually get involved, either blaming them (assuming they have been visiting porn sites) or making them change their e-mail or IM address.

Impersonation/Posing

Posing as the victim, the cyberbully can do considerable damage**.** While posing as the victim, they may post a provocative message in a hate group's chatroom or on their forum pages, inviting an attack against the victim, often giving the name, address, and telephone number of the victim to make the hate group's job easier. They often also send a message to someone saying hateful or threatening things while masquerading as the victim. They may also alter a message really from the victim, making it appear that they have said nasty things or shared secrets with others.

Social Networking Attacks

Most teens (and many preteens) are using social networks such as MySpace and Facebook. They build a profile and share whatever they want to share with the world or their close friends. They post pictures and videos (especially on video networks like YouTube), pass rumors, exclude those they want to target, create quizzes and polls, and use anonymous networks (such as JuicyCampus.com) or applications such as Honesty Box to attack their victims. They impersonate their victims, take over their accounts, or report them to their school, parents, or the police.

Aside from cellphones, social networking is the technology of choice for cyberbullying and harassment.

Misappropriation of Cellphones

While the predominant method used to cyberbully someone through a cellphone is texting and prank calling, students are lifting an unattended cellphone and reprogramming it to do their dirty work.

Cyberbullying by Proxy (Third Party Cyberharassment or Cyberbullying)

Often people who misuse the Internet to target others do it using accomplices. These accomplices, unfortunately, are often unsuspecting. They know they are communicating irate or provocative messages, but don't realize that they are being manipulated by the real cyberharasser or cyberbully. That's the beauty of this type of scheme. The attacker merely prods the issue by creating indignation or emotion on the part of others, and can then sit back and let others do their dirty work. Then, when legal action or other punitive actions are taken against the accomplice, the real attacker can claim that they never instigated anything and no one was acting on their behalf. They claim innocence and blame their accomplices, unwitting or not; their accomplices have no legal leg to stand on.

It's brilliant and very powerful. It is also one of the most dangerous kinds of cyberharassment or cyberbullying. Children do this often using AOL, MSN, or another ISP as their "proxy" or accomplice. When they engage in a "notify" or "warning" war, they are using this method to get the ISP to view the victim as the provocateur. A notify or warning war is when one child provokes another until the victim lashes back. When they do, the real attacker clicks the warning or notify button on the text screen. This captures the communication and flags it for the ISP's review. If the ISP finds that the communication violated their terms of service agreement (which most do), they may take action. Some accounts allow several warnings before formal action is taken, but the end result is the same. The ISP does the attacker's dirty work when they close or suspend the real victim's account for a terms of service violation. Most knowledgeable ISPs know this and are careful to see if the person being warned is really being set up.

Sometimes children use the victim's own parents as unwitting accomplices. They provoke the victim and, when the victim lashes back, they save the communication and forward it to the victim's parents. The parents often believe what they read and, without having evidence of the prior provocations, think that their own child "started it."

This works just as easily in a school disciplinary environment.

Students may not understand that their attacks, if designed to hurt someone's reputation, may be defamatory and subject them to discipline, lawsuits, and in some cases harassment charges. They may not understand that they can be tracked quite easily most of the time and held accountable for their actions. They may not understand that their actions may be a terms of service violation and cost them (or their family) their online accounts. They may repeat rumors and take action based on false information, and then find themselves facing liability when the person who started it all hides behind them. They should know that repeating lies, even if you read them online, is no excuse under the law.

WiredSafety advises not to respond to cyberbullying. So, it is important that we caution to all who believe things without confirming their accuracy not to confuse silence or failure to defend or rebut any rumors with an admission of guilt or confirmation that a lie told by someone is true. Sometimes silence is smarter, especially when the real fight may not occur online at all. The smarter ones don't fight their battles in public online, not when defamation, cyberbullying or harassment is involved.

Just a reminder to teach students to thinkB4uClick. Otherwise they have become what they say they are fighting. They have become a cyberharasser or cyberbully themselves. Teach them not to be used. Teach them to use their heads.

The Problem With Some Prominent Surveys

Major survey companies and educational institutions have studied cyberbullying. While they all conclude that cyberbullying is a serious and growing problem, they (in our opinion) under-report the problem. It's not their fault. It's the nature of how surveys with minors are conducted. Most take place after the parents are asked for their permission to survey their kids. Since there are 57 different reasons identified by students for why they would not tell their parents if targeted by a cyberbully, it is unlikely that they will be candid with the surveyor in their parents' presence or after their parents are informed about the survey.

The second problem with the surveys is that they ask, "Have you been cyberbullied?," without defining what they mean. Like "obscenity," which, according to a former U.S. Supreme Court Justice, "you know it when you see it," it's easier for people to spot than to define. But many students think that harassment and cruelty online comes with the territory, and unless it's a death threat or text-bomb (see Talk the Talk), it's not cyberbullying. For any survey to be effective, it needs to define situations that constitute cyberbullying and ask the students if they have ever been involved in one of those situations.

Interestingly, students are more likely to own up to being a cyberbully than a victim.

A Conspiracy to Conceal It

WiredSafety's surveys reflect that only 5% of students would tell their parents if they were being targeted by a cyberbully. When Teenangels conducted a survey of their own, they learned that less than 25% of the students would tell *anyone* if they were being cyberbullied.

Why? The answer is different for parents than another trusted adult. Parents have the power to make their lives miserable. They can turn off the Internet, take away cellphones, computers, and gaming devices, pick up the phone and call other parents, the school, or their lawyers. They run too hot and overreact, or too cold and underestimate the pain the cyberbully causes.

The students don't want their parents to discover that they are not as popular in school as hoped. They don't want to look like they can't take care of themselves. They don't want their parents to find out that they were doing things they shouldn't or to learn the information the cyberbully is threatening to expose.

Parents might start monitoring or filtering everything, spying, or being overly attentive to what the student is doing online. The parents may demand passwords to all accounts and use them, confront the cyberbully or their parents, call the police, or blow things out of proportion. The cyberbullying may become the topic of discussion over the Thanksgiving table or the source of teasing or bullying by siblings.

If their current or former friends were the cyberbullies, the victim, interestingly, may try and protect them or avoid having them punished. They don't want to be termed a "tattletale" or have the cyberbully

escalate their actions because they “told.” They may have responded using inappropriate language or threats of their own. The list goes on and on.

They are reluctant to share with their “friends” and not sure if the cyberbully is one of those in whom they are confiding. With anonymous cyberbullying they can’t be sure if the cyberbully is their best friend or worst enemy. Friends are armed with their secrets and passwords and sometimes the cyberbully poses as one of their friends. They don’t know where to turn or whom to trust.

Trusting their teachers, guidance counselors, and school administrators is a bit different. In this case, they worry that the school will refuse to get involved. (This fear is often well-founded.) They fear their uninformed involvement even more. When well-meaning school administrators get involved, they often call everyone in and try to get to the bottom of things. This only makes things worse and sets up the victim for more harassment from the cyberbully, their friends, and everyone in the class who sees the victim as “squealing.”

Even when the school administrators do the right thing, it can backfire. On a recent Tyra Banks Show, Parry met a young student who had reported her classmates taking her picture with their cellphone while in the locker room at school. (She and other girls were dancing in various stages of undress.) The cyberbully threatened to post the pictures on Facebook and the girl panicked and went to the principal, who promptly called in the girls and confiscated the cellphone. The entire class turned on the victim, saying she had blown it all out of proportion. She was victimized twice—once by the girls and again by the class.

An interesting exercise for students is to ask them to see how many reasons they can come up with why they wouldn’t tell their parents about being cyberbullied. Parry has never gotten them to come up with more than 57 different reasons. See if you can beat her record and share the reasons you find. They can be illuminating. If we understand why they don’t share this or trust their parents, we can find ways to address their concerns and change this pattern. We can also find ways to make sure that they trust guidance counselors, teachers, and school administrators so they don’t have to face this alone.

The challenge we all face is how we can intervene without feeding the cyberbullies. There are no easy answers on this one, just some approaches that have worked for others. An effective strategy is to get peer counselors involved and create a cyberbullying taskforce for the school, including students in crafting responses and consequences of cyberbullying activities. Make sure you include the consequences for bystanders.

Whatever you do, do it carefully and thoughtfully. Ask the victim first before you take any action other than those needed to protect them or others. Remember, cyberbullying hurts. The first thing we need to do is address that hurt. Bring in the guidance counselors to help. The more advance preparation and planning the school does, the faster and better you can respond when these things occur.

Starting Young - The Sumo Pandas

WiredSafety has created the Sumo Panda digital safety and cyberbullying prevention program to help teach cybersafety to kids from kindergarten to grade six. It uses a series of twelve short and cute Flash and Quicktime animations of the Pandas, their friends and rivals – the Polar Bears from Polar Bear

Academy. Each animation is paired with a teaching kit that contains things like lesson plans, activity sheets, coloring pages, pledges, and lesson certificates

Artemus and his cousin, Precious Panda live in the Forest of Kind with their families. Artemus and Precious attend Panda Elementary School with the other animals in their forest and love to sumo wrestle in their spare time! Like any other kid, they also love to play online. Too bad Artemus isn't the most cyber savvy and Precious often has to guide him to find the right path. Unfortunately, Artemus is often influenced by his "friends" Herbert the panda and Chops the pig who don't always have his best interests at heart. Artemus is also often the target of cyberbullying by his rivals, the Polar Bears from Polar Bear Academy. But with the support of his true friends, especially Precious, Artemus always learns important lessons in cybersafety by the end of the day.

Teaching them the consequences of their actions, and that the real "Men in Black" may show up at their front door sometimes helps too. Since many cyberbullying campaigns include some form of hacking or password or identity theft, serious laws are implicated. Law enforcement, including the FBI, might get involved in these cases. Remind your students that they could easily be implicated in a cyberbullying case commenced by one of their friends. (But be careful, this may end up backfiring if the kids are intrigued by what would happen if the FBI did knock on their door. It's happened.)

But few cyberbullying campaigns can succeed without the complacency and the often help of other kids. If no one votes at a cyber-bashing website, the cyberbully's attempts to humiliate the victim are thwarted. If no one forwards a hateful or embarrassing e-mail, the cyberbully is left standing all alone. It's rarely fun to act out unless you can show off to someone who will appreciate your antics. By denying the cyberbully an audience, the antics quickly stop.

In addition, the "mean girls" cyberbullies need an audience. That's the reason they do it, to show everyone that they *can*. It reinforces their social status and ranking. It reminds everyone who believes it that they can do anything they want to anyone they want. Denying them their audience and ego fix takes the fun out of cyberbullying. Hopefully they can then move on to something else a little less destructive.
If we can help kids understand how much bullying hurts, how in many cases (unlike the children's chant) words *can* hurt you, fewer may cooperate with the cyberbullies. They will think twice before forwarding a hurtful IM or e-mail, or visiting a cyberbullying "vote for the fat-girl" site, or allowing others to take videos or cell phone pictures of personal moments or compromising poses of others. And, in addition to not lending their efforts to continue the cyberbullying, if given an anonymous method of reporting cyberbullying websites, profiles and campaigns, students can help put an end to cyberbullying entirely. School administration, community groups and even school policing staff can receive these anonymous tips and take action quickly when necessary to shut down the site, profile or stop the cyberbullying itself. They can even let others know that they won't allow cyberbullying by supporting the victim, making it clear that they won't be used to torment others and that they care about the feelings of others is key. Martin Luther King, Jr. once said "In the end, we will remember not the words of our enemies, but the silence of our friends."

We need to teach our students that silence, when others are being hurt, is not acceptable. If they don't allow the cyberbullies to use them to embarrass or torment others, cyberbullying will quickly stop. It's a tall task, but a noble goal. And in the end, our students will be safer online and offline. We will have

helped create a generation of good cybercitizens, controlling the technology instead of being controlled by it.

APPENDIX ON RESPONSES TO MASSACHUSSET'S MIDDLE SCHOOL SURVEY OF 500 STUDENTS ON TEXTING - 2009

Student Survey - 770 Middle and High School Wisconsin Students Winter 2010

What do you know about cyberbullying?

	What is your grade?					
Answer Options	**6th**	**7th**	**8th**	**9th**	**10th**	**Response Percent**
I don't know what it is.	15	5	4	33	34	11.8%
It's no big deal.	1	3	2	39	24	9.0%
I have heard about it on TV or in magazines, but don't know much more.	4	17	17	63	42	18.6%
It happens in middle school only.	0	3	1	2	4	1.3%
It's when you say mean things online, in a text or by IM.	11	55	64	194	120	57.7%
It's when you take an embarrassing pic using a cell phone and send it to others to hurt someone.	11	47	64	144	70	43.6%
I have heard about someone in my school or town that was cyberbullied.	5	26	20	74	29	20.0%
Friends of mine have been cyberbullied, but I haven't.	4	17	7	35	16	10.3%
We've had cyberbullying incidents in my school.	3	21	16	69	29	17.9%
I have seen cyberbullying messages designed to hurt or embarrass someone else.	3	20	20	83	44	22.1%
I have cyberbullied others.	0	3	2	7	18	3.9%
I have said nasty things to others online, but don't consider it cyberbullying.	0	4	14	29	22	9.0%
I have been cyberbullied by a close friend.	1	9	4	23	13	6.5%
I have had someone steal my password and pretend to be me.	0	14	13	40	24	11.8%
I have had someone cyberbully me on Facebook.	0	5	4	18	14	5.3%
I have seen others cyberbullied on Facebook.	2	9	7	64	28	14.3%
I should report cyberbullying to the FBI.	0	20	5	20	8	6.9%
I know how to report cyberbullying to Facebook and other sites.	3	18	20	51	24	15.1%
You can be arrested if you cyberbully someone.	3	35	29	70	29	21.6%
Teens have committed suicide when they were cyberbullied.	5	46	60	138	57	39.7%
I've cyberbullied someone with my friends just for fun	0	1	6	20	12	5.1%
I have been harassed and embarrassed by text messages sent by others	2	11	15	33	15	9.9%